ELSEVIER

Discrete Mathematics 135 (1994) 377–379

DISCRETE MATHEMATICS

Note

On divisibility of binomial coefficients

Marko Razpet

University of Ljubljana, Institute of Mathematics, Physics and Mechanics, Department of Mathematics, Jadranska 19, 61 111 Ljubljana, Slovenia

Received 21 March 1989; revised 4 February 1993

Abstract

The Lucas theorem for binomial coefficients implies some interesting tensor product properties of certain matrices regarded for every prime p in the field $\mathscr{Z}_p$.

Let us define the array of numbers $C(i,j)$ for all nonnegative integers i and j by binomial coefficients:

$$C(i,j)=\binom{i}{j}.$$

We may display the numbers $C(i,j)$ as a matrix as follows:

$$\begin{pmatrix} C(0,0) & C(0,1) & C(0,2) & \cdots \\ C(1,0) & C(1,1) & C(1,2) & \cdots \\ C(2,0) & C(2,1) & C(2,2) & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 & \cdots \\ 1 & 1 & 0 & \cdots \\ 1 & 2 & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

The above matrix of entries $C(i,j)$ is the well-known left aligned Pascal triangle augmented by zeros on the right side. Let p be a prime. Denote by $C(i,j)_p$ the remainder of the division of $C(i,j)$ by p. The numbers $C(i,j)_p$ can be produced by Pascal identity calculating in the field $\mathscr{Z}_p$ (here $\mathscr{Z}$ denotes the ring of integers). The matrix of entries $C(i,j)_p$ also possesses several interesting properties; further, we can prove that $C(i,j)_p$ can be expressed by $C(i,j)_p$, $0\leqslant j<p$. To this end we define the principal matrix of order k as the finite matrix $A(k,p)$ with entries $C(i,j)_p$, $0\leqslant i<p^k$, $0\leqslant j<p^k$. In particular, we write $A(p)=A(1,p)$. We shall see that the principal matrix of order k is determined by the principal matrix of order 1 (cf. [2]). In other words, all information about the matrix of $C(i,j)_p$ is contained in the principal matrix of order 1.

SSDI 0012-365X(93)E0104-C

For any two matrices E and F the tensor (Kronecker) product $E \otimes F$ is defined as follows: the i,jth block of $E \otimes F$ is $e_{i,j}F$, where $e_{i,j}$ is the i,jth entry of E. The connection between principal cells gives the following theorem.

The Lucas theorem. *For each prime p and for every pair of nonnegative integers i and j is*

$$C(i,j) \equiv C(i_n, j_n)C(i_{n-1}, j_{n-1}) \cdots C(i_0, j_0) \pmod p,$$

where $i = i_n p^n + i_{n-1} p^{n-1} + \cdots + i_0$, $j = j_n p^n + j_{n-1} p^{n-1} + \cdots + j_0$, and $0 \leqslant i_k < p$, $0 \leqslant j_k < p$, $k = 0, 1, 2, \ldots, n$. (see, e.g., [1]).

The entries $a_{i,j}(n,p)$ of the matrix $A(m,p)$ can be expressed by the entries $a_{i,j}(p)$ of $A(p)$. We get from Lucas' theorem

$$a_{i,j}(n,p) \equiv a_{i_{n-1}, j_{n-1}}(p) a_{i_{n-2}, j_{n-2}}(p) \cdots a_{i_0, j_0}(p) \pmod p,$$

where $0 \leqslant i < p^n$, $0 \leqslant j < p^n$, and $i = i_{n-1} p^{n-1} + i_{n-2} p^{n-2} + \cdots + i_0$, $j = j_{n-1} p^{n-1} + j_{n-2} p^{n-2} + \cdots + j_0$ with $0 \leqslant i_k < p$, $0 \leqslant j_k < p$. The above relations prove:

For every integer $n \geqslant 1$ and every prime p the matrix $A(n,p)$ is the n-fold tensor product of the matrix $A(p)$ by itself in the field $\mathscr{Z}_p$.

We also observe the self-similarity of the array of numbers $C(i,j)_p$. Thus, the matrices $A(n,p)$ are self-similar and they can be calculated in $\mathscr{Z}_p$ by the Pascal identity. Each block $B_{i,j}(n,p) = a_{i,j}(p)A(n,p)$ satisfy the same recurrence relation as $a_{i,j}$ with respect to $\mathscr{Z}_p$.

Application. Using the above results we can count the nonzero entries of the matrix $A(n,p)$. This result is not new, but not so well-known (see [2]). The tensor product representation gives quickly the result.

Denote by $z(n,p)$ the number of all zero entries of the matrix $A(n,p)$ for a given integer $n \geqslant 1$ and a given prime p. Then the following formula holds:

$$z(n,p) = p^{2n} - \binom{p+1}{2}^n.$$

Indeed, considering separately tensor product blocks and counting the zero and nonzero entries of the matrix $A(p)$, we have a simple recurrence formula:

$$z(n+1,p) = z(n,p)[p^2 - z(1,p)] + z(1,p)p^{2n}.$$

Since

$$z(1,p) = 1 + 2 + \cdots + (p-1) = \binom{p}{2}$$

we get the desired result by induction.

The number of all nonzero entries of the matrix $A(n,p)$ is $p^{2n} - z(n,p) = \binom{p+1}{2}^n$. Since the array of $C(i,j)_p$ for $0 \leqslant j \leqslant i < p^n$ is Pascal's array modulo p, we see that the number of binomial coefficients $\binom{i}{j}$ for $0 \leqslant i < p^n$ which are not divisible by p is $\binom{p+1}{2}^n$.

If we mark black the points (i,j) if $C(i,j)$ is divisible by p, and white in other cases, then we obtain patterns of a very remarkable design.

Open problem 1. For the prime p find the minimal polynomial with coefficients in $\mathbb{Z}_p$ for the matrix $A(n,p)$ introduced above.

Open problem 2. Find double integer number array $N(i,j)$ which satisfies for every prime p the 'Lucas property':

$$N(i,j) \equiv N(i_n, j_n) N(i_{n-1}, j_{n-1}) \cdots N(i_0, j_0) \pmod p,$$

where $i = i_n p^n + i_{n-1} p^{n-1} + \cdots + i_0, j = j_n p^n + j_{n-1} p^{n-1} + \cdots + j_0$ with $0 \leqslant i_k < p$, $0 \leqslant j_k < p$ for $k = 0, 1, 2, \ldots, n$ in general form.

Acknowledgement

The author would like to thank Professor Marta Sved for helpful remarks.

References

[1] N. Fine, Binomial coefficients modulo a prime, Amer. Math. Monthly 54 (1947) 589–592.
[2] M. Sved, Divisibility — with visibility, The Math. Intelligencer 10 (1988) 56–64.